

**UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA**

MARC HARRELL, on behalf of himself
and all others similarly situated,

Plaintiff,

v.

**ALLIANZ LIFE INSURANCE
COMPANY OF NORTH AMERICA**, a
Minnesota corporation.

Defendant.

Case No.:

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff Marc Harrell (“Plaintiff”) brings this class action on behalf of himself, and all others similarly situated, against Defendant, Allianz Life Insurance Company of North America (“Allianz Life” or “Defendant”), alleging as follows based upon information and belief and investigation of counsel, except as to the allegations specifically pertaining to them, which are based on personal knowledge:

NATURE OF THE ACTION

1. This class action arises out of Defendant’s failures to properly secure and safeguard potentially thousands of Class Members’ sensitive personal identifiable information (“PII” or “Private Information”).

2. Defendant’s data security failures led to a detection of suspicious activity and breach in their network systems (the “Data Breach”) that, upon information and belief, contained the Private Information of Plaintiff and other individuals (“the Class”). The date of the Data Breach has not been disclosed by Defendant nor the number of affected

individuals, but Defendant released a Notice to impacted individuals, including Plaintiff, on June 13, 2025. *See* **Exhibit A**.

3. Upon information and belief, an unauthorized third party accessed Defendant's network systems between 2024 and 2025 and obtained Plaintiff's and Class Member's Private Information.

4. Defendant is an insurance company that provides a comprehensive range of insurance products and services and annuities to its clients.

5. Upon information and belief, the Private Information compromised in the Data Breach included certain personal information—such as names, dates of birth, home addresses, phone numbers, insurance policy numbers, and Social Security Numbers—of individuals whose Private Information was maintained by Defendant, including Plaintiff.

6. PII has great value to cyber criminals, especially Social Security numbers. As a direct cause of Defendant's Data Breach, Plaintiff and the Class's PII is potentially in the hands of cyber-criminals and may be available for sale on the dark web for other criminals to access and abuse at the expense of Plaintiff and the Class. Plaintiff and the Class face a current and lifetime risk of imminent identity theft or fraud as a direct result of the Data Breach.

7. Defendant acknowledged the severity of the Data Breach and the value of PII and has provided impacted individuals with identity monitoring services by Kroll, including Triple Bureau Credit monitoring, Web Watcher monitoring, fraud consultation, and identity theft restoration.

8. Defendant has numerous statutory, regulatory, contractual, and common law

duties and obligations, including those based on its affirmative representations to Plaintiff and the Class, to keep their PII confidential, safe, secure, and protected from unauthorized disclosure or access.

9. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect individuals' Private Information with which it was entrusted.

10. Upon information and belief, the mechanism of the Data Breach and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure Private Information from those risks left that property in a dangerous condition.

11. Upon information and belief, Defendant breached its duties and obligations by failing, in one or more of the following ways: (1) failing to design, implement, monitor, and maintain reasonable network safeguards against foreseeable threats; (2) failing to design, implement, and maintain reasonable data retention policies; (3) failing to adequately train staff on data security; (4) failing to comply with industry-standard data security practices; (5) failing to warn Plaintiff and Class Members of Defendant's inadequate data security practices; (6) failing to encrypt or adequately encrypt the Private Information; (7) failing to recognize or detect that its network had been compromised and accessed in a timely manner to mitigate the harm; (8) failing to utilize widely available software able to detect and prevent this type of attack, and (9) otherwise failing to secure the hardware using reasonable and effective data security procedures free of foreseeable

vulnerabilities and data security incidents.

12. Defendant impliedly understood its obligations and promised to safeguard Plaintiff's and Class Members' Private Information. Plaintiff and Class Members relied on these implied promises when seeking out and paying for Defendant's services. But for this mutual understanding, Plaintiff and Class Members would not have provided Defendant with their Private Information. Defendant, however, did not meet these reasonable expectations, causing Plaintiff and Class Members to suffer injury.

13. Defendant disregarded the rights of Plaintiff and Class Members (defined below) by, *inter alia*, intentionally, willfully, recklessly, and/or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard Plaintiff's and Class Members' Private Information; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiff(s) and Class Members with prompt and full notice of the Data Breach.

14. In addition, Defendant failed to properly monitor the computer network and systems that housed the Private Information. Had it properly monitored its property, it would have discovered the intrusion sooner.

15. Upon information and belief, Plaintiff's and Class Members' identities are now at risk because of Defendant's negligent conduct since the Private Information that Defendant collected and maintained is now potentially in the hands of data thieves.

16. As a result of the Data Breach, Plaintiff and Class Members are now at a

current, imminent, and ongoing risk of fraud and identity theft. Plaintiff and Class Members must now and for years into the future closely monitor their insurance and financial accounts to guard against identity theft. As a result of Defendant's unreasonable and inadequate data security practices, Plaintiff and Class Members have suffered numerous actual and concrete injuries and damages.

17. The risk of identity theft is not speculative or hypothetical but is impending and has materialized as there is evidence that the Plaintiff's and Class Members' Private Information was targeted, accessed, has been misused, and potentially disseminated on the Dark Web.

18. Plaintiff and Class Members must now closely monitor their financial accounts to guard against future identity theft and fraud. Plaintiff and Class Members have heeded such warnings to mitigate against the imminent risk of future identity theft and financial loss. Such mitigation efforts included and will continue to include in the future, among other things: (a) reviewing financial statements; (b) reviewing insurance policy statements; (c) changing passwords; and (c) signing up for credit and identity theft monitoring services. The loss of time and other mitigation costs are tied directly to guarding against the imminent risk of identity theft.

19. Plaintiff and Class Members have suffered numerous actual and concrete injuries as a direct result of the Data Breach, including: (a) financial costs incurred mitigating the materialized risk and imminent threat of identity theft; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft; (c) deprivation of value of their PII; and (d) the continued risk to their

sensitive Private Information, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect it collected and maintained.

20. Through this Complaint, Plaintiff seeks to remedy these harms on behalf of himself and all similarly situated individuals whose Private Information was accessed during the Data Breach.

21. Accordingly, Plaintiff brings this action against Defendant seeking redress for its unlawful conduct and asserting claims for: (i) negligence and negligence *per se*, (ii) breach of implied contract, (iii) breach of fiduciary duty, (iv) unjust enrichment, and (v) declaratory relief.

22. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, as well as long-term and adequate credit monitoring services funded by Defendant, and declaratory relief.

23. The exposure of one's Private Information to cybercriminals is a bell that cannot be un-rung. Before this Data Breach, Plaintiff's and the Class's Private Information was exactly that—private. Not anymore. Now, their Private Information is forever exposed and unsecure.

PARTIES

24. Plaintiff Marc Harrell is an adult individual who at all relevant times has been a citizen and resident of Orlando, Florida.

25. Defendant Allianz is a stock insurance corporation with its principal place of

business located at 5701 Golden Hills, Drive, Minneapolis, MN 55416. Defendant conducts business through this District, the State of Minnesota, and the United States.

JURISDICTION AND VENUE

26. This Court has diversity jurisdiction over this action under the Class Action Fairness Act (CAFA), 28 U.S.C. § 1332(d), because this is a class action involving more than 100 class members, the amount in controversy exceeds \$5,000,000, exclusive of interest and costs, and Class Members are citizens of states that differ from Defendant.

27. This Court has personal jurisdiction over Defendant because Defendant conducts business in and has sufficient minimum contacts with Florida.

28. Venue is likewise proper as to Defendant in this District under 28 U.S.C. § 1391(a)(1) because Defendant's principal place of business is in this District and many of Defendant's acts complained of herein occurred within this District.

FACTUAL BACKGROUND

A. Defendant Knew the Risks of Storing Valuable Private Information and the Foreseeable Harm to Victims.

29. At all relevant times, Defendant knew it was storing and permitting its employees to use its internal network server to transmit valuable, sensitive Private Information and that, as a result, Defendant's systems would be attractive targets for cybercriminals.

30. Defendant also knew that any breach of its systems, and exposure of the information stored therein, would result in the increased risk of identity theft and fraud against the individuals whose Private Information was compromised, as well as intrusion

into their highly private life insurance information.

31. These risks are not merely theoretical; in recent years, numerous high-profile breaches have occurred at businesses such as Equifax, Yahoo, Marriott, Anthem, and many others.

32. The Private Information compromised in the Data Breach has considerable value and constitutes an enticing and well-known target to hackers. Hackers easily can sell stolen data as a result of the “proliferation of open and anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce.”¹

33. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities in the U.S. According to the ITRC, in Q1 of 2024, there were 841 total reported data breaches in the United States.²

34. The breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Defendant’s clients especially vulnerable to identity theft, tax fraud, insurance fraud, credit and bank fraud, and more.

35. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches: “[I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data has been sold

¹ Brian Krebs, *The Value of a Hacked Company*, Krebs on Security (July 14, 2016), <http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/> (last visited Aug. 27, 2024).

² *Identity Theft Resource Center Q1 2024 Data Breach Analysis: Compromises Up 90 Percent Over Q1 2023*, IDENTITY THEFT RESOURCE CENTER, available at <https://www.idtheftcenter.org/post/q1-2024-data-breach-analysis-compromises-up-90-percent-over-q1-2023/>.

or posted on the [Dark] Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.”³

36. Even if stolen Private Information does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained Private Information about the individual, such as names, addresses, email addresses, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

B. Defendant Breached its Duty to Protect its Customers’ Private Information.

37. Defendant agreed to and undertook legal duties to maintain the protected personal information entrusted to it by Plaintiff and Class Members safely, confidentially, and in compliance with all applicable laws, including the Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45. Under state and federal law, businesses like Defendant have duties to protect client’s Private Information and to notify them about breaches.

38. The Private Information held by Defendant in its computer system and network included the highly sensitive Private Information of Plaintiff and Class Members.

39. Although Defendant has not disclosed the nature of the Data Breach,

³ United States Government Accountability Office, Report to Congressional Requesters, Personal Information, June 2007: <https://www.gao.gov/assets/gao-07-737.pdf> (last visited July 3, 2025).

including the date(s) it detected suspicious activity in its network systems or the number of individuals potentially affected, Defendant sent notice of the incident on June 26, 2025.

40. The Data Breach occurred as a direct result of Defendant's failure to implement and follow basic security procedures, and its failure to follow its own policies, in order to protect its customers' Private Information.

41. Omitted from the Notice Letter were the root cause of the Data Breach, the vulnerabilities exploited, and the number of individuals potentially affected. To date, these omitted details have not been explained or clarified to Plaintiff and Class Members, who retain a vested interest in ensuring that their Private Information remains protected.

42. Upon information and belief, the cyberattack was targeted at Defendant, due to its status as a life insurance and annuities entity that collects, creates, and maintains Private Information on its computer networks and/or systems.

43. In response to the Data Breach, Defendant informed Plaintiff and Class Members in its June 2025 Notice about identity fraud protection services offered by Kroll.

44. As evidenced by the Data Breach's occurrence, the Private Information contained in Defendant's network was not encrypted. Had the information been properly encrypted, the data thieves would have exfiltrated only unintelligible data.

C. Defendant Failed to Comply with the FTC Guidelines.

45. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

46. In 2022, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their networks' vulnerabilities; and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.⁴

47. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

48. The FTC has brought enforcement actions against businesses for failing to protect consumer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential customer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the

⁴ Ritchie, J.N. & A., & Jayanti, S.F.-T. and A. (2022, April 26). Protecting personal information: a guide for business. Federal Trade Commission.

measures businesses must take to meet their data security obligations.

49. Defendant failed to properly implement basic data security practices.

50. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to customers' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

51. To prevent and detect cyber-attacks, Defendant could and should have implemented, as recommended by the United States Government and FTC, the following measures:

- a. implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of malware and how it is delivered;
- b. enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing;
- c. scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users;
- d. configure firewalls to block access to known malicious IP addresses;
- e. patch operating systems, software, and firmware on devices. Consider using a centralized patch management system;
- f. set anti-virus and anti-malware programs to conduct regular scans automatically;
- g. manage the use of privileged accounts based on the principle of least privilege; no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary;
- h. configure access controls—including file, directory, and network share

permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares;

- i. disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications;
- j. implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common malware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData Folder;
- k. consider disabling Remote Desktop protocol (RDP) if it is not being used;
- l. use application whitelisting, which only allows systems to execute programs known and permitted by security policy;
- m. execute operating system environments or specific programs in a virtualized environment; and
- n. categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.

52. Upon information and belief, Defendant was at all times fully aware of its obligation to protect the Private Information of its customers. Defendant was also aware of the significant repercussions that would result from its failure to do so.

D. Defendant Failed to Comply with Industry Standards

53. A number of industry and national best practices have been published and should have been used as a go-to resource and authoritative guide when developing Defendant's cybersecurity practices. Best cybersecurity practices that are standard in the financial services industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management

systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

54. Upon information and belief, Defendant failed to meet the minimum standards of the following cybersecurity frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established standards in reasonable cybersecurity readiness. These frameworks are existing and applicable industry standards in Defendant's industry, and Defendant failed to comply with these accepted standards, thereby opening the door to the cyber-attack and causing the Data Breach.

55. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent ransomware attacks, resulting in the Data Breach.

E. Plaintiff and Class Members' Damages

56. For the reasons mentioned above, Defendant's conduct, which allowed the Data Breach to occur, caused Plaintiff and Class Members significant injuries and harm in several ways. Plaintiff and Class Members must immediately devote time, energy, and money to: 1) closely monitor their life insurance statements, bills, records, and credit and financial accounts; 2) change login and password information on any sensitive account even more frequently than they already do; 3) more carefully screen and scrutinize phone

calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and 4) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

57. Once Private Information is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiff and Class Members will need to maintain these heightened measures for years, and possibly their entire lives, as a result of Defendant's conduct. Further, the value of Plaintiff's and Class Members' Private Information has been diminished by its exposure in the Data Breach.

58. As a result of Defendant's failures, Plaintiff and Class Members are at substantial increased risk of suffering identity theft and fraud or misuse of Private Information.

59. Plaintiff and the Class Members have been injured by Defendant's unauthorized disclosure of their confidential and private information.

60. Plaintiff and Class Members are also at a continued risk because their information remains in Defendant's systems, which have already been shown to be susceptible to compromise and attack and are subject to further attacks so long as Defendant fails to undertake the necessary and appropriate security and training measures to protect its customers' Private Information.

F. Plaintiff's Experience

61. Plaintiff is a customer of Allianz Life Insurance Company.

62. In order to obtain services, Defendant required Plaintiff's name, date of birth,

Social Security number, address, email address, and other sensitive information. Defendant stored this information on its unsecured network.

63. On or around June 13 2025, Plaintiff received an email from Defendant notifying him that Allianz Life detected suspicious activity that may have resulted in the compromise of his information (“Notice”).

64. As a result of the Data Breach, Plaintiff’s sensitive information may have been accessed and/or acquired by an unauthorized actor. The confidentiality of Plaintiff’s sensitive information has been irreparably harmed. For the rest of his life, Plaintiff will have to worry about when and how his sensitive information may be shared or used to his detriment.

65. As a result of the Data Breach, Plaintiff spent time dealing with the consequences of the Data Breach, which includes times spent verifying the legitimacy of the Data Breach and self-monitoring his accounts. This time has been lost forever and cannot be recaptured.

66. Additionally, Plaintiff is very careful about not sharing his sensitive PII. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

67. Plaintiff stores any documents containing his sensitive PII in safe and secure locations or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

68. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and experiences fear and anxiety and increased concern for the

loss of his privacy.

69. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII being placed in the hands of unauthorized third parties and possibly criminals.

70. Plaintiff has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

COMMON INJURIES AND DAMAGES

71. As result of Defendant's ineffective and inadequate data security practices, Plaintiff and Class Members now face a present and ongoing risk of fraud and identity theft.

72. Due to the Data Breach, and the foreseeable consequences of Private Information ending up in the possession of criminals, the risk of identity theft to Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including but not limited to: (a) invasion of privacy; (b) "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) loss of time due to increased spam and targeted marketing emails; (e) the loss of benefit of the bargain (price premium damages); (f) diminution of value of their Private Information; and (g) the continued risk to their Private Information, which remains in Defendant's possession, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate

measures to protect Plaintiff's and Class Members' Private Information.

A. The Risk of Identity Theft to Plaintiff and Class Members is Present and Ongoing

73. Plaintiff and members of the proposed Class have suffered injury from the misuse of their PII that can be directly traced to Defendant.

74. Defendant negligently disclosed the PII of Plaintiff and the Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII of Plaintiff and the Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII.

75. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

76. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity – or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

77. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as “social engineering” to obtain even more information

about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data breaches are often the starting point for these additional targeted attacks on the victims.

78. The dark web is an unindexed layer of the Internet that requires special software or authentication to access.⁵ Criminals in particular favor the dark web as it offers a degree of anonymity to visitors and website publishers. Unlike the traditional or 'surface' web, dark web users need to know the web address of the website they wish to visit in advance. For example, on the surface web, the CIA's web address is `cia.gov`, but on the dark web the CIA's web address is `ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion`.⁶ This prevents dark web marketplaces from being easily monitored by authorities or accessed by those not in the know.

79. A sophisticated black market exists on the dark web where criminals can buy or sell malware, firearms, drugs, and frequently, and personal information like the Private Information at issue here.⁷ The digital character of PII stolen in data breaches lends itself to dark web transactions because it is immediately transmissible over the Internet and the

⁵ *What Is the Dark Web?*, Experian, available at <https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/> (last visited July 3, 2025).

⁶ *Id.*

⁷ *What is the Dark Web?* – Microsoft 365, available at <https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web> (last visited July 3, 2025).

buyer and seller can retain their anonymity. The sale of a firearm or drugs on the other hand requires a physical delivery address. Nefarious actors can readily purchase usernames and passwords for online streaming services, stolen financial information and account login credentials, and Social Security numbers, dates of birth, and medical information.⁸ As Microsoft warns “[t]he anonymity of the dark web lends itself well to those who would seek to do financial harm to others.”⁹

80. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to numerous serious fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual’s Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don’t pay the bills, it damages your credit. You may not find out that someone is using your number until you’re turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.¹⁰

81. What’s more, it is no easy task to change or cancel a stolen Social Security

⁸ *Id.*; *What Is the Dark Web?*, Experian, available at <https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/> (last visited July 3, 2025).

⁹ *What is the Dark Web?* – Microsoft 365, available at <https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web> (last visited July 3, 2025).

¹⁰ Social Security Administration, *Identity Theft and Your Social Security Number*, available at: <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last visited July 3, 2025).

number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

82. Even then, a new Social Security number may not be effective, as “[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number.”¹¹

83. Identity thieves can also use Social Security numbers to obtain a driver’s license or official identification card in the victim’s name but with the thief’s picture; use the victim’s name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim’s information. In addition, identity thieves may obtain a job using the victim’s Social Security number, rent a house or receive medical services in the victim’s name, and may even give the victim’s personal information to police during an arrest resulting in an arrest warrant being issued in the victim’s name. And the Social Security Administration has warned that identity thieves can use an individual’s Social Security number to apply for additional credit lines.¹²

84. According to the FBI’s Internet Crime Complaint Center (IC3) 2019 Internet

¹¹ Brian Naylor, *Victims of Social Security Number Theft Find It’s Hard to Bounce Back*, NPR (Feb. 9, 2015), <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft> (last visited July 3, 2025).

¹² *Identity Theft and Your Social Security Number*, Social Security Administration, 1 (2018), <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last visited July 3, 2025).

Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than \$3.5 billion in losses to individuals and business victims.¹³

85. Further, according to the same report, “rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good.”¹⁴ Defendant did not rapidly report to Plaintiff and the Class that their Private Information had been stolen.

86. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

87. In addition to out-of-pocket expenses that can exceed thousands of dollars, and the emotional toll identity theft can take, some victims must spend a considerable time repairing the damage caused by the theft of their Private Information. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

88. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen Private Information. To protect themselves, Plaintiff and Class Members will need to remain vigilant against unauthorized

¹³ See <https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120> (last visited July 3, 2025).

¹⁴ *Id.*

data use for years or even decades to come.

89. The FTC has also recognized that consumer data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that “most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis and profit.”¹⁵

90. The FTC has also issued numerous guidelines for businesses that highlight the importance of reasonable data security practices. The FTC has noted the need to factor data security into all business decision-making. According to the FTC, data security requires: (1) encrypting information stored on computer networks; (2) retaining payment card information only as long as necessary; (3) properly disposing of personal information that is no longer needed; (4) limiting administrative access to business systems; (5) using industry-tested and accepted methods for securing data; (6) monitoring activity on networks to uncover unapproved activity; (7) verifying that privacy and security features function properly; (8) testing for common vulnerabilities; and (9) updating and patching third-party software.¹⁶

91. According to the FTC, unauthorized disclosures of Private information are

¹⁵ Statement of FTC Commissioner Pamela Jones Harbour (Remarks Before FTC Exploring Privacy Roundtable), <http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf> (last visited July 3, 2025).

¹⁶ See generally <https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business> (last visited July 3, 2025).

extremely damaging to consumers' finances, credit history and reputation, and can take time, money and patience to resolve the fallout. The FTC treats the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5(a) of the FTC Act.¹⁷

92. Defendant's failure to notify Plaintiff and Class Members of the Data Breach exacerbated Plaintiff's and Class Members' injury by depriving them of the earliest ability to take appropriate measures to protect their Private Information and take other necessary steps to mitigate the harm caused by the Data Breach.

B. Loss of Time to Mitigate the Risk of Identify Theft and Fraud

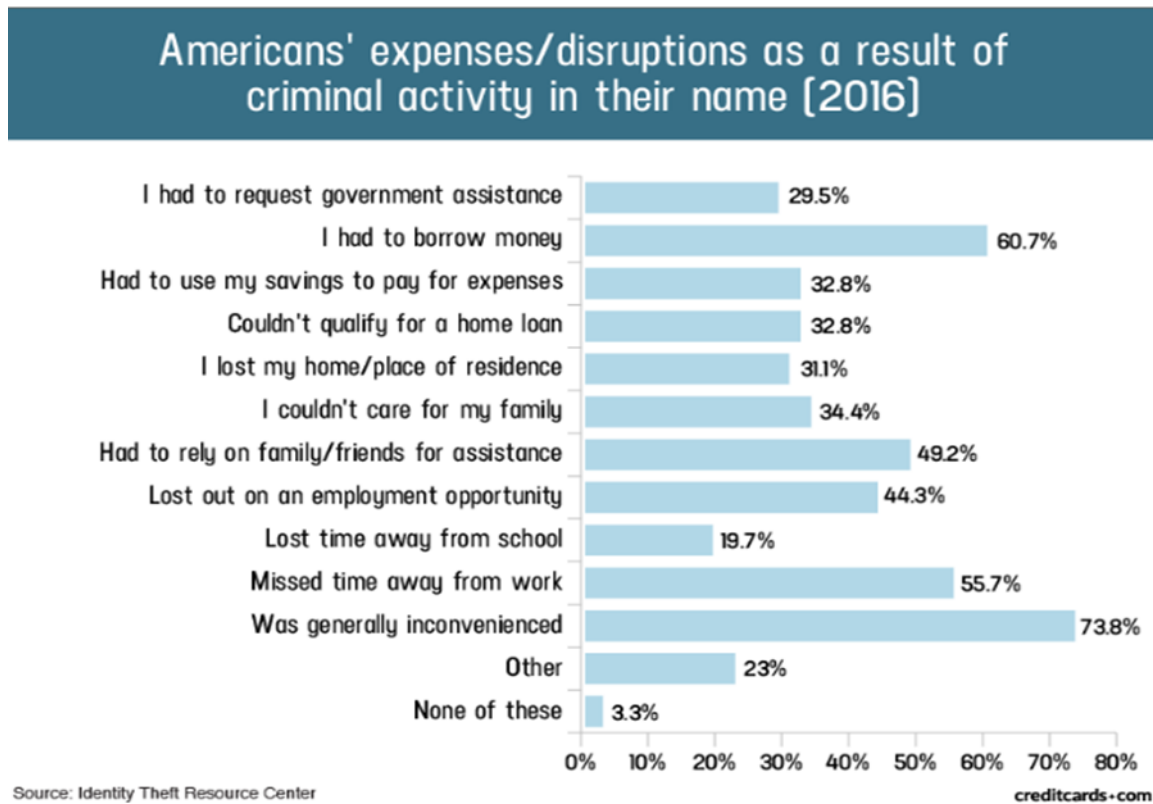
93. As a result of the recognized risk of identity theft, when a data breach occurs, and an individual is notified by a company that their Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft or fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet, the resource and asset of time has been lost.

94. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as placing “freezes” and “alerts” with credit reporting agencies, contacting financial institutions, closing or modifying financial accounts, changing passwords, reviewing and monitoring credit reports and accounts for

¹⁷ See, e.g., <https://www.ftc.gov/news-events/news/press-releases/2016/07/commission-finds-labmd-liable-unfair-data-security-practices> (last visited July 3, 2025).

unauthorized activity, and filing police reports, which may take years to discover and detect.

95. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:¹⁸



96. In the event that Plaintiff and Class Members experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches (“GAO Report”) in which it noted that victims of identity theft will face “substantial costs and time to repair the damage to their good name and credit

¹⁸ “Credit Card and ID Theft Statistics” by Jason Steele, 10/24/2017, at <https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php>.

record.”¹⁹ Indeed, the FTC recommends that identity theft victims take several steps and spend time to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.²⁰

C. Diminution of Value of the Private Information

97. PII is a valuable property right.²¹ Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

98. Private Information can sell for as much as \$363 per record according to the Infosec Institute.²²

99. An active and robust legitimate marketplace for Private Information also

¹⁹ See “Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown,” p. 2, U.S. Government Accountability Office, June 2007, <https://www.gao.gov/new.items/d07737.pdf> (“GAO Report”) (last visited July 3, 2025).

²⁰ See <https://www.identitytheft.gov/Steps> (last visited July 3, 2025).

²¹ See, e.g., John T. Soma, et al, Corporate Privacy Trend: The “Value” of Personally Identifiable Information (“PII”) Equals the “Value” of Financial Assets, 15 Rich. J.L. & Tech. 11, at *1 (2009) (“PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.”) (citations omitted).

²² See Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), <https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/> (last visited July 3, 2025).

exists. In 2019, the data brokering industry was worth roughly \$200 billion.²³ In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.^{24, 25} Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to \$50 a year.²⁶

100. As a result of the Data Breach, Plaintiff's and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished in its value by its unauthorized release onto the Dark Web.

D. Future Cost of Credit and Identify Theft Monitoring is Reasonable and Necessary

101. Given the type of targeted attack in this case and sophisticated criminal activity, the type of Private Information involved, and the volume of data obtained in the Data Breach, entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes –e.g., opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

102. Such fraud may go undetected until debt collection calls commence months,

²³ See <https://www.latimes.com/business/story/2019-11-05/column-data-brokers> (last visited July 3, 2025).

²⁴ See <https://datacoup.com/> (last visited July 3, 2025).

²⁵ See <https://digi.me/what-is-digime/> (last visited July 3, 2025).

²⁶ Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at <https://computermobilepanel.nielsen.com/ui/US/en/faqs.html> (last visited July 3, 2025).

or even years, later. An individual may not know that his or her personal information was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

103. Consequently, Plaintiff and Class Members are at a present and continuous risk of fraud and identity theft for many years into the future.

104. The retail cost of credit monitoring and identity theft monitoring can cost around \$200 a year per Class Member. This is a reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach. This is a future cost for a minimum of five years that Plaintiff and Class Members would not need to bear but for Defendant's failure to safeguard their Private Information.

E. Loss of Benefit of the Bargain

105. Furthermore, Defendant's poor data security deprived Plaintiff and Class Members of the benefit of their bargain. When agreeing to provide their Private Information, which was a condition precedent to obtain services, and paying Defendant for its services, Plaintiff as a consumer understands and expected that he was, in part, paying for services and data security to protect the Private Information required to be collected from him.

106. In fact, Defendant did not provide the expected data security. Accordingly, Plaintiff and Class Members received services that were of a lesser value than what he reasonably expected to receive under the bargains struck with Defendant.

F. Injunctive Relief is Necessary to Protect Against Future Data Breaches

107. Moreover, Plaintiff and Class Members have an interest in ensuring that Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing Private Information is not accessible online and that access to such data is password protected.

108. Because of Defendant's failure to prevent the Data Breach, Plaintiff and Class members suffered—and will continue to suffer—damages. These damages include, *inter alia*, monetary losses and lost time. Also, Plaintiff and Class Members suffered or are at an increased risk of suffering:

- a. loss of the opportunity to control how their Private Information is used;
- b. diminution in value of their Private Information;
- c. compromise and continuing publication of their Private Information;
- d. out-of-pocket costs from trying to prevent, detect, and recovery from identity theft and fraud;
- e. lost opportunity costs and wages from spending time trying to mitigate the fallout of the Data Breach by, *inter alia*, preventing, detecting, contesting, and recovering from identify theft and fraud;
- f. delay in receipt of tax refund monies;
- g. unauthorized use of their stolen Private Information; and
- h. continued risk to their Private Information—which remains in Defendant's possession—and is thus at risk for futures breaches so long as Defendant fails to take appropriate measures to protect the Private Information.

CLASS ALLEGATIONS

109. Plaintiff brings this case individually and, pursuant to Federal Rule of Civil Procedure 23, on behalf of the following Class:

All individuals in the United States whose Private Information was compromised in the Defendant's Data Breach.

110. Excluded from the Class is Defendant, its subsidiaries and affiliates, its officers, directors and members of their immediate families and any entity in which Defendant has a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

111. Plaintiff reserves the right to modify or amend the definition of the proposed Class prior to moving for class certification.

112. **Numerosity.** The class described above is so numerous that joinder of all individual members in one action would be impracticable. The disposition of the individual claims of the respective Class Members through this class action will benefit both the parties and this Court. It is believed the class size consists of potentially thousands of class members. The exact size of the Class and the identities of the individual members thereof are ascertainable through Defendant's records, including but not limited to, the files implicated in the Data Breach.

113. **Commonality.** This action involves questions of law and fact that are common to the Class Members. Such common questions include, but are not limited to:

- a. whether Defendant had a duty to protect the Private Information of Plaintiff and Class Members;

- b. whether Defendant had a duty to maintain the confidentiality of Plaintiff and Class Members' Private Information;
- c. whether Defendant breached its obligation to maintain Plaintiff and the Class Members' life insurance information in confidence;
- d. whether Defendant was negligent in collecting, storing and safeguarding Plaintiff's and Class Members' Private Information, and breached its duties thereby;
- e. whether Defendant breached its fiduciary duty to Plaintiff and the Class;
- f. whether Plaintiff and Class Members are entitled to damages as a result of Defendant's wrongful conduct;
- g. whether Plaintiff and Class Members are entitled to restitution or disgorgement as a result of Defendant's wrongful conduct; and
- h. whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

114. **Typicality.** Plaintiff's claims are typical of the claims of the Class Members. The claims of the Plaintiff and members of the Class are based on the same legal theories and arise from the same failure by Defendant to safeguard Private Information. Plaintiff and Class Members were all customers of Defendant, each having their Private Information obtained by an unauthorized third party.

115. **Adequacy of Representation.** Plaintiff is an adequate representative of the Class because his interests do not conflict with the interests of the other Class Members he seeks to represent; Plaintiff has retained counsel competent and experienced in complex class action litigation; Plaintiff intends to prosecute this action vigorously; and Plaintiff's counsel has adequate financial means to vigorously pursue this action and ensure the

interests of the Class will not be harmed. Furthermore, the interests of the Class Members will be fairly and adequately protected and represented by Plaintiff and Plaintiff's counsel.

116. **Predominance.** Common questions of law and fact predominate over any questions affecting only individual Class Members. For example, Defendant's liability and the fact of damages is common to Plaintiff and each member of the Class. If Defendant breached its common law and statutory duties to secure Private Information on its network server, then Plaintiff and each Class Member suffered damages from the exposure of sensitive Private Information in the Data Breach.

117. **Superiority.** Given the relatively low amount recoverable by each Class Member, the expenses of individual litigation are insufficient to support or justify individual suits, making this action superior to individual actions.

118. **Manageability.** The precise size of the Class is unknown without the disclosure of Defendant's records. The claims of Plaintiff and the Class Members are substantially identical as explained above. Certifying the case as a class action will centralize these substantially identical claims in a single proceeding and adjudicating these substantially identical claims at one time is the most manageable litigation method available to Plaintiff and the Class.

FIRST CAUSE OF ACTION
NEGLIGENCE AND NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Class)

119. Plaintiff restates and realleges all proceeding allegations above as if fully set forth herein.

120. Defendant owed a duty under common law to Plaintiff and Class Members

to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

121. Defendant's duty to use reasonable care arose from several sources, including but not limited to those described below.

122. Defendant had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices on the part of Defendant. By collecting and storing Private Information that is routinely targeted by criminals for unauthorized access, Defendant was obligated to act with reasonable care to protect against these foreseeable threats.

123. Defendant's duty also arose from Defendant's position as a provider of life insurance. Defendant holds itself out as a trusted provider of life insurance and thereby assumes a duty to reasonably protect its customer's information. Indeed, Defendant, as an insurance provider, was in a unique and superior position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

124. Defendant breached the duties owed to Plaintiff and Class Members and thus was negligent. Defendant breached these duties by, among other things: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of Private Information; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks;

(c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; and (g) failing to follow its own privacy policies and practices published to its customers.

125. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, their Private Information would not have been compromised.

126. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by entities such as Defendant or failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendant's duty.

127. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect the Private Information and not complying with the industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of a data breach involving the Private Information of its customers.

128. Plaintiff and members of the Class are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

129. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

130. The harm that has occurred as a result of Defendant's conduct is the type of

harm that the FTC Act was intended to guard against.

131. Defendant violated its own policies not to use or disclose Private Information without written authorization.

132. Defendant violated its own policies by actively disclosing Plaintiff's and the Class Members' Private Information; by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information; failing to maintain the confidentiality of Plaintiff's and the Class Members' records; and by failing to provide timely notice of the breach of Private Information to Plaintiff and the Class.

133. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered injuries, including:

- a. theft of their Private Information and publishing of such information to the dark web;
- b. costs associated with the detection and prevention of identity theft and unauthorized use of financial accounts;
- c. costs associated with purchasing credit monitoring and identity theft protection services;
- d. lowered credit scores resulting from credit inquiries following fraudulent activities;
- e. costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Defendant Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;
- f. the imminent and certainly impending injury flowing from the increased

risk of potential fraud and identity theft posed by their Private Information being placed in the hands of criminals;

- g. damages to and diminution in value of their Private Information entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiff's and Class Members' data against theft and not allow access and misuse of their data by others;
- h. continued risk of exposure to hackers and thieves of their Private Information, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' data;
- i. loss of their privacy and confidentiality in their Private Information;
- j. the erosion of the essential and confidential relationship between Defendant – as a life insurance and annuities provider – and Plaintiff and Class Members as customers; and
- k. loss of personal time spent carefully reviewing life insurance policy and annuities statements.

134. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

SECOND CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class)

135. Plaintiff restates and realleges all proceeding allegations above as if fully set forth herein.

136. When Plaintiff and members of the Class provided their Private Information to Defendant, Plaintiff and members of the Class entered into implied contracts with Defendant pursuant to which Defendant agreed to safeguard and protect such information

and to timely and accurately notify Plaintiff and Class Members that their data had been breached and compromised.

137. Defendant required Plaintiff and Class Members to provide and entrust their Private Information as a condition of obtaining Defendant's services.

138. Plaintiff and Class Members would not have provided and entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant.

139. Plaintiff and members of the Class fully performed their obligations under the implied contracts with Defendant.

140. Defendant breached the implied contracts it made with Plaintiff and Class Members by failing to safeguard and protect the Private Information of Plaintiff and members of the Class and by failing to provide timely notice to them that their Private Information was compromised in and as a result of the Data Breach.

141. As a direct and proximate result of Defendant's breach of the implied contracts, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, and/or disgorgement or restitution, in an amount to be proven at trial.

THIRD CAUSE OF ACTION
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff and the Class)

142. Plaintiff restates and realleges all proceeding allegations above as if fully set forth herein.

143. Plaintiff and Class Members have an interest, both equitable and legal, in the

Private Information about them that was conveyed to, collected by, and maintained by Defendant and that was ultimately accessed or compromised in the Data Breach.

144. As a life insurance provider, Defendant has a fiduciary relationship to its customers, like Plaintiff and the Class Members.

145. Because of that fiduciary relationship, Defendant was provided with and stored private and valuable Private Information related to Plaintiff and the Class, which it was required to maintain in confidence.

146. Defendant owed a fiduciary duty under common law to Plaintiff and Class Members to exercise the utmost care in obtaining, retaining, securing, safeguarding, deleting, and protecting their Private Information in its possession from being compromised, lost, stolen, accessed by, misused by, or disclosed to unauthorized persons.

147. As a result of the parties' fiduciary relationship, Defendant had an obligation to maintain the confidentiality of the information within Plaintiff and the Class Members' insurance records.

148. Customers like Plaintiff and Class Members have a privacy interest in personal life insurance matters, and Defendant had a fiduciary duty not to disclose insurance data concerning its customers.

149. As a result of the parties' relationship, Defendant had possession and knowledge of confidential Private Information of Plaintiff and Class Members, information not generally known.

150. Plaintiff and Class Members did not consent to nor authorize Defendant to release or disclose their Private Information to an unknown criminal actor.

151. Defendant breached the duties owed to Plaintiff and Class Members by, among other things: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of Private Information; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; (g) failing to follow its own privacy policies and practices published to its customers; and (h) making an unauthorized and unjustified disclosure and release of Plaintiff and the Class members' PII and life insurance records/information to a criminal third party.

152. But for Defendant's wrongful breach of its fiduciary duties owed to Plaintiff and Class Members, their privacy, confidences, and Private Information would not have been compromised.

153. As a direct and proximate result of Defendant's breach of its fiduciary duties and breach of its confidences, Plaintiff and Class Members have suffered injuries, including:

- a. theft of their Private Information and publication of such information to the dark web;
- b. costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts;

- c. costs associated with purchasing credit monitoring and identity theft protection services;
- d. lowered credit scores resulting from credit inquiries following fraudulent activities;
- e. costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Defendant Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;
- f. the imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their Private Information being placed in the hands of criminals;
- g. damages to and diminution in value of their Private Information entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiff's and Class Members' data against theft and not allow access and misuse of their data by others;
- h. continued risk of exposure to hackers and thieves of their Private Information, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' data;
- i. loss of their privacy and confidentiality in their Private Information;
- j. the erosion of the essential and confidential relationship between Defendant – as a life insurance and annuities provider – and Plaintiff and Class Members as customers; and
- k. loss of personal time spent carefully reviewing statements from life insurance policies and annuities to check for unauthorized changes.

154. As a direct and proximate result of Defendant's breach of its fiduciary duty, Plaintiff and Class Members are entitled to damages, including compensatory, punitive,

and/or nominal damages, in an amount to be proven at trial.

FOURTH CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

155. Plaintiff restates and realleges all proceeding allegations above as if fully set forth herein.

156. This count is brought in the alternative to Plaintiff's breach of implied contract count.

157. Plaintiff and Class Members conferred a benefit on Defendant by way of customers paying Defendant to maintain Plaintiff and Class Members' Private Information.

158. The monies paid to Defendant were supposed to be used by Defendant, in part, to pay for the administrative and other costs of providing reasonable data security and protection to Plaintiff and Class Members.

159. Defendant failed to provide reasonable security, safeguards, and protections to the personal information of Plaintiff and Class Members, and as a result Defendant was overpaid.

160. Under principles of equity and good conscience, Defendant should not be permitted to retain the money because Defendant failed to provide adequate safeguards and security measures to protect Plaintiff's and Class Members' Private Information that they paid for but did not receive.

161. Defendant wrongfully accepted and retained these benefits to the detriment of Plaintiff and Class Members.

162. Defendant's enrichment at the expense of Plaintiff and Class Members is and

was unjust.

163. As a result of Defendant's wrongful conduct, as alleged above, Plaintiff and the Class are entitled to restitution and disgorgement of profits, benefits, and other compensation obtained by Defendant, plus attorneys' fees, costs, and interest thereon.

FIFTH CAUSE OF ACTION
DECLARATORY JUDGMENT
(On Behalf of Plaintiff and the Class)

164. Plaintiff restates and realleges all proceeding allegations above as if fully set forth herein.

165. This Court is authorized to declare rights, status, and other legal relations, and such declarations shall have the force and effect of a final judgment or decree. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

166. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and Class Members' Private Information and whether Defendant is currently maintaining data security measures adequate to protect Plaintiff and Class Members from further data breaches that compromise their Private Information. Plaintiff alleges that Defendant's data security measures remain inadequate, contrary to Defendant's assertion that it has confirmed the security of its network. Furthermore, Plaintiff continues to suffer injury as a result of the compromise of Private Information and remains at imminent risk that further compromises of Private Information will occur in the future.

167. Pursuant to its authority, this Court should enter a judgment declaring, among other things, the following:

- a. Defendant owes a legal duty to secure Private Information and to timely notify customers or any individuals impacted of a data breach under the common law, Section 5 of the FTC Act, HIPAA, various state statutes, and the common law; and
- b. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure consumers' Private Information.

168. This Court also should issue corresponding prospective injunctive relief requiring Defendant to, at minimum 1) disclose, expeditiously, the full nature of the Data Breach and the types of Private Information accessed, obtained, or exposed by the hackers; 2) implement improved data security practices to reasonably guard against future breaches of Plaintiff and Class Members' Private Information possessed by Defendant; and 3) provide, at its own expense, all impacted victims with lifetime identity theft protection services.

169. If an injunction is not issued, Plaintiff will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Defendant. The risk of another such breach is real, immediate, and substantial. If another breach at Defendant occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantified, and they will be forced to bring multiple lawsuits to rectify the same conduct.

170. The hardship to Plaintiff if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued. Plaintiff will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively

minimal, and Defendant has a pre-existing legal obligation to employ such measures.

171. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Defendant, thus eliminating the additional injuries that would result to Plaintiff and Class Members whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all other similarly situated, pray for relief as follows:

- a. for an order certifying the Class under Federal Rule of Civil Procedure 23 and naming Plaintiff as the representative of the Class and Plaintiff's attorneys as Class Counsel to represent the Class;
- b. for an order finding in favor of Plaintiff and the Class on all counts asserted herein;
- c. for compensatory, statutory, treble, and/or punitive damages in amounts to be determined by the trier of fact;
- d. for an order of restitution, disgorgement, and all other forms of equitable monetary relief;
- e. declaratory and injunctive relief as described herein;
- f. awarding Plaintiff's reasonable attorneys' fees, costs, and expenses;
- g. awarding pre- and post-judgment interest on any amounts awarded; and
- h. awarding such other and further relief as may be just and proper.

JURY TRIAL DEMANDED

A jury trial is demanded on all claims so triable.

Dated: July 8, 2025

Respectfully Submitted,

/s/ Bryan Bleichner

Bryan Bleichner (#0326689)

Philip Krzeski (#0403291)

CHESTNUT CAMBRONNE

100 Washington Ave. South

Minneapolis, MN 55401

Telephone: (612) 339-7300

Facsimile: (612) 336-2940

bbleichner@chestnutcambronne.com

pkrzeski@chestnutcambronne.com

Jeff Ostrow (*pro hac vice* forthcoming)

Steven Sukert (*pro hac vice* forthcoming)

KOPELOWITZ OSTROW P.A.

1 W. Las Olas Blvd., Suite 500

Fort Lauderdale, FL 33301

Telephone: (954) 525-4100

ostrow@kolawyers.com

sukert@kolawyers.com

***Counsel for Plaintiff and the Putative
Class***